UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/020,308	12/18/2001	Masato Yamamichi	2001_1845A	8418

513 7590 11/15/2005

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/020,308	YAMAMICHI ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on September 01, 2005. All claims 1-19 have been amended.

Response to Arguments

2. Applicant's argument filed on September 01, 2005 have been fully considered but they are not persuasive.

The first argument by the applicant is about the independent claims and applicant argued that it includes limitations that are not shown or suggested by the references on the record, namely **Dai.**

Applicant wrote the following in support of his argument, "If the Examiner considers that "W = hI (x) xor M" corresponds to the encrypting means of claims 1 and 18 or the encrypting operation of claims 15-17, then Dai cannot be interpreted as an disclosing any operation or circuitry remotely resembling a first operation means for performing an invertible operation on the plaintext (M) and the first additional information to generate connected information, as recited in claims 1 and 18, or performing an invertible operation on the plaintext (M) and the first additional information to generate connected information, as recited in claims 15-17"

Examiners disagrees with the above argument,

For the sake of clarity every independent claim has to be seen independently, the argument made by the applicant does not specifically address how the reference used failed to disclose the limitation of the independent claims.

Examiner however would point out that Dai the reference on the record discloses the following, the transmission apparatus [Encoder, shown on figure 3 and figure 1] **encrypting plaintext to generate ciphertext, performing a one-way operation on the plaintext to generate a first value, transmitting the ciphertext and the first value to the reception apparatus,** [figure 3, ref. "104", ref. Num "106" and ref. Num "108"] (The first value is met to be h2 (x, M) which is generated by performing a one-way hash function on the plain text M, and the ciphertext is met to be C shown on figure 3, ref. Num "106" which is the result of the plaintext after it is encrypted.)

Therefore the cipher text C has two components a value V and a value W as explained on column 2, lines 31-55

The ciphertext C disclosed by the reference meets the limitation of an invertible operation on the plaintext and the first additional information to generate connected information and is not patentably distinguishable from the applicant encrypting means of claims 1 and 18 or the encrypting operation of claims 15-17. [See the office action below]

The scope of the limitation of the claims is not changed by the amendment and Examiner asserts that Dai discloses the claimed limitations and the rejection is maintained.

Therefore all the elements of the limitations is explicitly or implicitly suggested and disclosed by the references on the records and the rejection remains valid.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. **Claims 1 and 3-19** are rejected under 35 U.S.C. 102(e) as being anticipated by Wel Dai (hereinafter referred as **Dai**)(U.S. Patent 6,081,598)

5. **As per claims 1,3-4,6-19 Dia discloses a**

- **Cryptocommunication system including a transmission apparatus and a reception apparatus wherein,** [figure 1 and 3, ref. "Encoder" and " Decoder"]
- **Said transmission apparatus** [Encoder, shown on figure 3 and figure 1] **is operable to encrypt plaintext to generate ciphertext, perform a one-way operation on the plaintext to generate a first value, and transmit the ciphertext and the first value to said reception apparatus,** [figure 3, ref. "104", ref. Num "106" and ref. Num "108"] (The first value is met to be h2 (x, M) which is generated by performing a one-way hash function on the plain text M, and the ciphertext is met to be C shown on figure 3, ref. Num "106" which is the result of the plaintext after it is encrypted.)
- **Said reception apparatus is operable to receive the ciphertext and the first value, decrypt the ciphertext to generate decrypted text,[figure 3, ref. Num "112"] perform the one-way operation on the decrypted text to generate a second value,**[figure 3, ref. Num 114, see h2' (x, M)] and
- **Judge that Pull the decrypted text matches the plaintext when the second value and the first value match,** [figure 3. ref. Num "114", see comparing the second hash value with the first hash value]

- **Said transmission apparatus comprises**: [figure 1 and 3, reference "Encoder"]

- **First generating means for generating first additional information;** [Column 2, lines 31-47; figure 3, ref. Num "V"] (The ciphertext C has , a value V and a value W and the first additional information is met to be "X").

- **First operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information; encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext;** [column 2, lines 31-47 and column 2, lines 48-50; Figure 3, ref. Num "102" see "cipehertext"] and

Transmitting means for transmitting the ciphertext, [Figure 3, ref. Num "106" and figure 1, ref. Num "26"] and

Said reception apparatus comprising: [Figure 3, reference "Decoder" and figure 1, ref. Num "24"]

- **Receiving means for receiving the ciphertext transmitted from said transmitting means;** [figure 3, ref. Num "108" see "C"]

- **Second generating means for generating second additional information which is identical to the first additional information generated by said first generating means**; [Figure 3, ref. Num "110"]

- **Decrypting means for decrypting the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm so as to generate decrypted connected information; and second operation means for performing an inverse operation of the invertible operation on the decrypted connected information and the second**

additional information so as to generate the decrypted text. [Column 2, lines 53-63]

6. **As per claims 5 Dia discloses a cryptocommunication system as applied to claim 1 above. Furthermore Dia discloses the system wherein** said first generating means generates a random number, and sets the generated random number as the first additional information.[Column 2, lines 43-44]

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claim 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over Wel Dai (hereinafter referred as **Dai**)(U.S. Patent 6,081,598) in view of Michael F. Jones. (hereinafter referred to as Jones) (U.S. Patent 5,412,730)

9. **As per claim 2, Dai** discloses a cryptocommunication system generating the first additional information and second additional information. [Column 2, lines 31-43, See "X" and also see figure 3, ref. Num "110"]

Dai does not explicitly disclose said second generating means synchronizes with said first generation means so as to generate the second additional information which is identical to the first additional information.

However, in the same field of endeavor, **Jones** discloses the second generating means synchronizes with the first generation means so as to generate the second information which is identical to the first information.[column 1, lines 37-53]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of generating the same value at the transmitting and receiving station in synchronism as per teachings of Jones in to the method taught by Dai, in order to securely monitor the follow of transmission and be able to decode all of the transmitted information. [See Jones, Column 1, lines 34-36]

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
11/02/2005

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100